ManageEngine
DataSecurity Plus

A unified data visibility and security platform

- File Audit
- File Analysis
- Data Risk Assessment
- Data Leak Prevention
- Cloud Protection

Agenda

About DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It provides the below capabilities:

- File server auditing
- File integrity monitoring
- Ransomware detection and response
- Security incident response
- File and security permission analysis
- Data discovery and classification
- File copy protection
- Endpoint data leak prevention
- Cloud application protection, and more.

Solutions offered

DataSecurity Plus comprises of the below modules:

File Audit

Report, analyze, and alert on file accesses and modifications in real time

File Analysis

Analyze file storage, monitor disk space usage, and examine security permissions to locate junk data and security vulnerabilities

Data Risk Assessment

Discover and classify files containing sensitive data (PII, PCI, and ePHI)

Data Leak Prevention

Detect and disrupt sensitive data leaks via endpoints (USBs, email, etc.)

Cloud Protection

Audit your organization's web traffic to track and control the use of high-risk web applications

Download now

Highlights of

File Audit

Highlights of File Audit

- **Audit file and folder access**: Track file read, create, modify, move, delete, copy, paste, etc. to learn who did what, when, and from where

- **Monitor file integrity:** Detect critical events like file changes after business hours, user activity in sensitive files, and multiple failed access attempts

- **Receive real-time change alerts:** Alert admins to unauthorized or unusual file changes, and automatically execute custom scripts to shut down attacks

- **Shut down ransomware attacks:** Detect and respond to ransomware attacks with an automated threat response mechanism

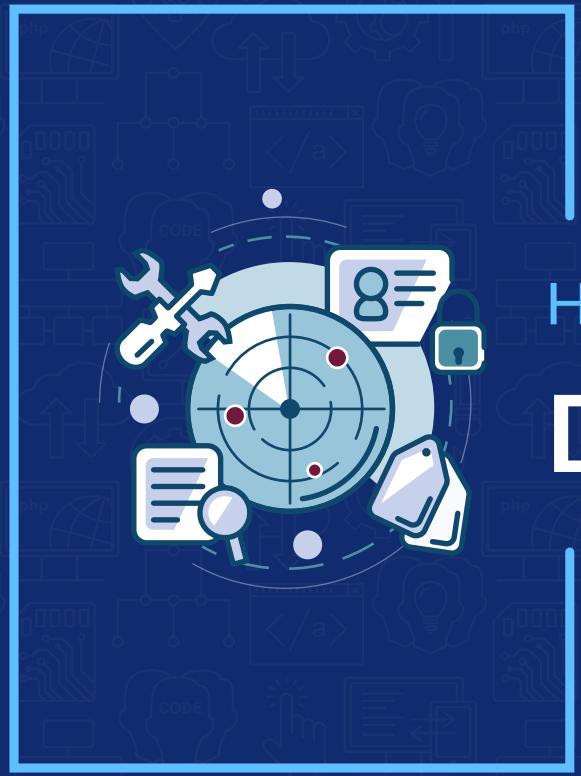
- **Comply with regulatory mandates:** Meet the requirements of multiple IT regulations like PCI DSS, HIPAA, GDPR, FISMA, GLBA, and more

Highlights of

File Analysis

Highlights of File Analysis

- **Manage ROT data:** Find and delete redundant, obsolete, and trivial files to reduce expenditure on storage
- **Delete duplicate files:** Locate duplicate files by comparing file names, sizes, and last modification times, and delete the unnecessary copies to free up primary storage
- **Analyze disk space usage:** Track disk space consumption, and receive alerts on critically low disk space to ensure business continuity
- **Examine file permissions:** Analyze NTFS permissions and detect security vulnerabilities like broken inheritances and files owned by dormant users
- **Detect overexposed files:** Detect files with excessive permissions such as those accessible by every user or allow unrestricted access



Highlights of

Data Risk Assessment

Highlights of Data Risk Assessment

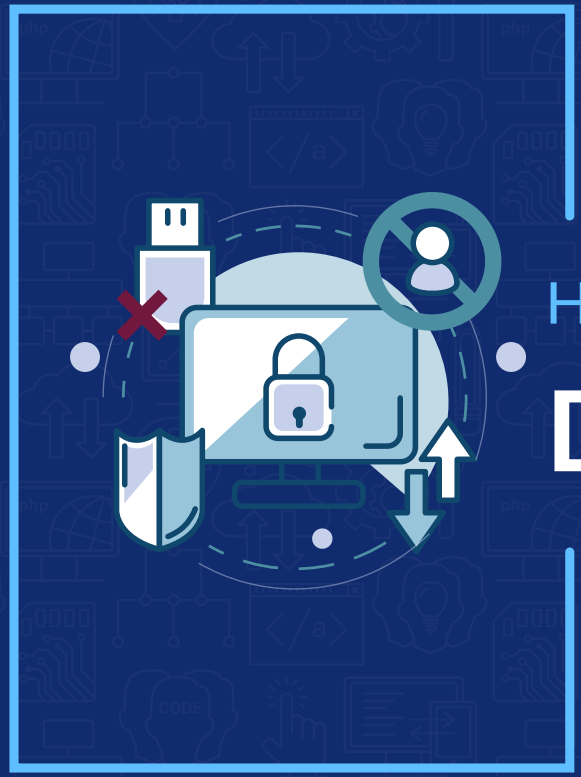
- **Discover sensitive data:** Scan enterprise storage for passport numbers, email addresses, credit card numbers, and over fifty other types of personal data
- **Analyze trends in PII storage:** Receive reports on the volume, type, and trends in the storage of sensitive data
- **Detect storage policy violations:** Instantly detect data that violates enterprise storage policies and respond by executing custom script
- **Analyze file sensitivity and vulnerability:** Analyze the risk associated with files by viewing details on the amount and type of personal data they contain and who can access them
- **Classify sensitive files:** Classify files containing PII, PCI, or ePHI to better understand which files need elevated data security measures

- **Avoid non-compliance:** Avoid the risk of non-compliance penalties by generating periodic reports on the location and amount of sensitive data stored in your environment

- **Leverage incremental scanning:** Scan only new and recently modified files to reduce data discovery scan times

- **Examine file security:** Identify employees who can access files containing personal information

- **Analyze risk scores:** Assess the vulnerability of personal data with an evolving risk score, assigned based on its content, ownership, and more



Highlights of

Data Leak Prevention

Highlights of Data Leak Prevention

- **Audit file activity in endpoints:** Audit file accesses across your Windows workstations in real time
- **Classify endpoint data:** Classify files based on their sensitivity as Public, Internal, Confidential, or Restricted
- **Enable content-aware protection:** Closely monitor who owns and accesses sensitive data. Execute instant responses when threats to this data are detected
- **Monitor removable devices:** Audit and control the use of removable storage media and all sensitive data transfer activities to them
- **Prevent data leaks via USBs:** Lock down peripheral ports in response to malicious user behavior to prevent potential data leaks

Block data exfiltration via email: Block files with highly sensitive data—such as PII or ePHI—from being moved via email (Outlook)

Automate incident response: Delete or quarantine files, block USB ports, or choose from other predefined remediation options to prevent data leaks

Audit printer usage: Track and analyze who printed what files and when

Control the use of applications: Create allow and block lists to exercise granular control over which applications can be used by employees

Prevent file copy actions: Track attempts to copy critical files across local and network shares and block unwarranted file transfers

Highlights of

Cloud Protection

Highlights of Cloud Protection

- **Track cloud application usage:** Monitor your organization's web traffic to analyze the use of sanctioned or unsanctioned apps

- **Assess the threat of shadow IT:** Spot employees who are putting your organization at risk with their use of shadow cloud applications

- **Monitor web requests:** Capture all HTTP requests along with details on when a cloud application was accessed, by whom, the app's reputation details, and more

- **Block unsanctioned applications:** Prevent your employees from accessing or uploading corporate data via high-risk applications by blocking their actions in real time

Licensing details

File Audit

Licensed based on the number of file servers. Users also get 1TB free File Analysis capabilities for every licensed server.

File Analysis

Licensed based on data size in Terabytes.

Data Risk Assessment

Licensed based on data size in Terabytes.

Data Leak Prevention

Licensed based on the number of endpoints.

Cloud Protection

Free add-on of the Data Leak Prevention module.

Supported platforms

File Audit

Windows File Server 2003 R2 and above

File Analysis

Windows File Server 2003 R2 and above

Data Risk Assessment

Windows File Server 2003 and above

Data Leak Prevention

Windows XP and above

Cloud Protection

Windows XP and above, Windows Server 2003 and above, Linux, and Mac

How we aid your evaluation

- A fully functional 30-day, free trial
- Extension of evaluation license, if needed
- 24x5 technical support
- An online demo hosted at demo.datasecurityplus.com
- An extensive knowledge base

Our customers

DataSecurity Plus is a high valued solution that ensures file system integrity and data loss prevention, and it helps us comply with regulatory standards.

Phurich Leemakanot, Mubadala Petroleum

Contact us

Telephone
+1.925.924.9500

Live chat
For instant responses.

Email the support team
support@datasecurityplus.com

Visit our website
www.datasecurityplus.com

Mailing address
ZOHO Corporation, 4141 Hacienda Drive,
Pleasanton, CA 94588, USA

Download now